Available online at www.sciencedirect.com
SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 579–590
European Journal of Combinatorics
www.elsevier.com/locate/ejc

# A family of group character codes

San Ling

*Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Singapore*

Received 1 November 2002; accepted 1 June 2003

**Abstract**

In IEEE Trans. Inform. Theory 46 (2000), 280, using characters of an elementary Abelian 2-group, a class of $q$-ary codes, where $q$ is an odd prime power, is constructed. These codes share several features in common with binary Reed–Muller codes. This construction is generalized in this paper to yield codes with features that resemble those of generalized Reed–Muller codes.


*Keywords:* Generalized Reed–Muller codes; Matrix-product codes; Group character codes; Vandermonde determinant

## 1. Introduction

A class of group character codes $C_q(r, n)$, defined over $\mathbf{F}_q$, where $q$ is an odd prime power, was constructed in [4] using characters of elementary Abelian 2-groups. These codes have parameters $[2^n, \sum_{i=0}^{r} \binom{n}{i}, 2^{n-r}]$, which are similar to those for binary Reed–Muller codes. It was also shown in loc. cit. that the dual of $C_q(r, n)$ is equivalent to $C_q(n - r - 1, n)$, again similar to a property of binary Reed–Muller codes.

In this paper, we consider a similar construction where the group used is $(\mathbf{Z}/p\mathbf{Z})^n$, for any positive integer $p$. We show that the group character codes obtained in this case bear some similarities with the generalized Reed–Muller codes in terms of their parameters and their duals. The method used to obtain our results is more general than those in [4]. It turns out that these group character codes are matrix-product codes in the sense of [1], so some results of [1] are used in our study of these codes.

*E-mail address:* lings@math.nus.edu.sg (S. Ling).

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.06.002

## 2. Basic definitions

For any positive integer $p$, write the elements of $(\mathbf{Z}/p\mathbf{Z})^n$ as $(a_1, \ldots, a_n)$, where $0 \le a_i \le p-1$ for each $1 \le i \le n$.

Let $\mathbf{F}_q$ denote a finite field that contains a $p$th root of unity, i.e., $p$ divides $q-1$. Let $\zeta$ be a fixed $p$th root of unity in $\mathbf{F}_q$. It is well-known from the theory of group characters that there are exactly $p^n$ distinct characters of $(\mathbf{Z}/p\mathbf{Z})^n$ with values in $\mathbf{F}_q^*$. In fact, these characters can be described very explicitly in the following manner.

Every $j$ such that $0 \le j \le p^n - 1$ has a unique $p$-adic expansion of the form

$$j = \sum_{i=1}^{n} j_i p^{i-1},$$

where $0 \le j_i \le p-1$ for all $1 \le i \le n$.

**Lemma 1.** *The group characters from $(\mathbf{Z}/p\mathbf{Z})^n$ to $\mathbf{F}_q^*$ are precisely $f_0, f_1, \ldots, f_{p^n-1}$, where*

$$f_j((a_1, \ldots, a_n)) = \zeta^{a_1 j_1 + \cdots + a_n j_n}.$$

**Proof.** It is clear that $f_j$ is a character from $(\mathbf{Z}/p\mathbf{Z})^n$ to $\mathbf{F}_q^*$, for every $0 \le j \le p^n - 1$ and that they are distinct. Furthermore, since there are exactly $|(\mathbf{Z}/p\mathbf{Z})^n| = p^n$ distinct characters from $(\mathbf{Z}/p\mathbf{Z})^n$ to $\mathbf{F}_q^*$, they are all accounted for by $f_0, \ldots, f_{p^n-1}$. □

**Definition.** For $a = (a_1, \ldots, a_n) \in (\mathbf{Z}/p\mathbf{Z})^n$, where $0 \le a_i \le p-1$ for each $1 \le i \le n$, let $\|a\|$ denote the sum $a_1 + \cdots + a_n$ as a *rational integer*, i.e.,

$$\|a\| = a_1 + \cdots + a_n \in \mathbf{Z}.$$

**Remark.** Note that, in particular, $0 \le \|a\| \le (p-1)n$ for all $a \in (\mathbf{Z}/p\mathbf{Z})^n$.

**Definition.** For all integers $r$, let

$$X(r, n; p) = \{a \in (\mathbf{Z}/p\mathbf{Z})^n : \|a\| > r\}.$$

**Remark.** In particular, $X(r, n; p) = (\mathbf{Z}/p\mathbf{Z})^n$ for all $r < 0$, and $X(r, n; p) = \emptyset$ for all $r \ge n(p-1)$.

**Definition.** With $\mathbf{F}_q$ as above and $\zeta \in \mathbf{F}_q^*$ a fixed $p$th root of unity, for a given integer $r$, let $C_q(r, n; p)$ denote the $q$-ary code

$$C_q(r, n; p) = \left\{ (c_0, c_1, \ldots, c_{p^n-1}) \in \mathbf{F}_q^{p^n} : \sum_{j=0}^{p^n-1} c_j f_j(x) = 0 \quad \text{for all } x \in X(r, n; p) \right\}.$$

**Remark.** Note that $C_q(r, n; 2)$ is exactly the code $C_q(r, n)$ of [4].

Clearly, $C_q(r, n; p)$ is a linear code of length $p^n$. We will show that $C_q(r, n; p)$ is a matrix-product code defined in [1] and use this fact to analyze the code. In order for this exposition to be self-contained, we recall briefly here some definitions and facts related to matrix-product codes (cf. [1] for more details).

**Definition.** Let $M = (m_{ij})$ be an $\ell \times N$ matrix with entries in $\mathbf{F}_q$ and let $C_1, \ldots, C_\ell$ be codes of length $m$ over $\mathbf{F}_q$. The **matrix-product code** $(C_1 \ldots C_\ell)M$ is the set of all matrix products $(\mathbf{c}_1 \ldots \mathbf{c}_\ell)M$, where $\mathbf{c}_i \in C_i$ is an $m \times 1$ column vector for $i = 1, \ldots, \ell$, and the entries of the matrix $(\mathbf{c}_1 \ldots \mathbf{c}_\ell)M$ are read in a column-major order. In other words, writing $\mathbf{c}_i = (c_{1i}, c_{2i}, \ldots, c_{mi})^{\mathrm{T}}$ for $1 \le i \le \ell$, the word $(\mathbf{c}_1 \ldots \mathbf{c}_\ell)M$ is $(c'_1, c'_2, \ldots, c'_{mN})$, where, for $1 \le j \le m$ and $1 \le k \le N$,

$$c'_{(k-1)m+j} = c_{j1}m_{1k} + \cdots + c_{j\ell}m_{\ell k}.$$

For $1 \le t \le \ell$, let $M_t$ denote the matrix consisting of the first $t$ rows of $M$ and, for $1 \le j_1 \le \cdots \le j_t \le N$, write $M(j_1, \ldots, j_t)$ for the $t \times t$ matrix consisting of the columns $j_1, \ldots, j_t$ of $M_t$.

**Definition.** An $\ell \times N$ matrix $M$ is **non-singular by columns (NSC)** if $M(j_1, \ldots, j_t)$ is non-singular for each $1 \le t \le \ell$ and $1 \le j_1 \le \cdots \le j_t \le N$.

**Proposition 2** ([1, Theorem 3.7]). *If $M$ is NSC and $C = (C_1 \ldots C_\ell)M$, then*

(i) $|C| = |C_1| \cdots |C_\ell|$;
(ii) $d(C) \ge d^* = \min(Nd_1, (N-1)d_2, \ldots, (N-\ell+1)d_\ell)$, *where $d(C), d_1, \ldots, d_\ell$ are the minimum distances of $C, C_1, \ldots, C_\ell$, respectively; and*
(iii) *if $M$ is the column-permutation of an upper triangular matrix, then $d(C) = d^*$.*

## 3. Properties of $C_q(r, n; p)$

We have seen that, for all $r < 0$, we have $X(r, n; p) = (\mathbf{Z}/p\mathbf{Z})^n$ and hence $C_q(r, n; p) = \{\mathbf{0}\}$. Similarly, for all $r \ge n(p-1)$, we have $X(r, n; p) = \emptyset$ and hence $C_q(r, n; p) = \mathbf{F}_q^{p^n}$. Therefore, for the rest of this paper, we often restrict our attention to the case $0 \le r < n(p-1)$.

We begin our study of the properties of the codes $C_q(r, n; p)$ by looking at their length and dimension.

**Proposition 3.** *For $0 \le r < n(p-1)$, the code $C_q(r, n; p)$ has length $p^n$ and dimension $s_n(r)$, where*

$$s_n(r) = \sum_{i=0}^{r} \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n-1+i-kp}{n-1}.$$

**Proof.** It is clear from the definition that the length of $C_q(r, n; p)$ is $p^n$.

Denote the elements of $X(r, n; p)$ by $x_i (1 \le i \le |X(r, n; p)|)$. From the orthogonality relations of group characters (cf. [4, Lemma 1]), it is easy to see that the rows of the matrix $H = (f_{j-1}(x))_{x \in X(r,n;p), 1 \le j \le p^n}$ are linearly independent. Hence, $H$ is a parity check matrix for $C_q(r, n; p)$, implying that the dimension of $C_q(r, n; p)$ is $p^n - |X(r, n; p)|$.

Let $\binom{n}{i}_p$ denote the number of elements $a$ of $(\mathbf{Z}/p\mathbf{Z})^n$ such that $\|a\| = i (0 \le i \le n(p-1))$. Then clearly the dimension of $C_q(r, n; p)$ is

$$p^n - |X(r, n; p)| = \sum_{i=0}^{r} \binom{n}{i}_p.$$

It is known (cf. [3, p. 216]) that

$$\binom{n}{i}_p = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n-1+i-kp}{n-1},$$

so the proposition follows. □

**Theorem 4.** *For $0 \le r \le n(p-1)$, the code $C_q(r, n; p)$ is the matrix-product code $(C_1 \dots C_p)M$, where $C_i = C_q(r+1-i, n-1; p)$ for $1 \le i \le p$ and $M = (m_{ij})$ is the $p \times p$ matrix with the entries given by*

$$m_{ij} = (-1)^{j-i} \zeta^{\frac{1}{2}(j-i+1)(j-i)} \prod_{k=j-i+1}^{p-i} (\zeta^k - 1) \Big/ \prod_{\ell=1}^{p-j} (\zeta^\ell - 1), \tag{1}$$

*for $1 \le i, j \le p$. (The empty product is taken to be 1.)*

**Proof.** We first claim that

$$\dim(C_q(r, n; p)) = \sum_{i=1}^{p} \dim(C_q(r+1-i, n-1; p)). \tag{2}$$

We shall then show that

$$(C_1 \dots C_p)M \subseteq C_q(r, n; p). \tag{3}$$

Thus, combining (2) and (3), it follows that $C_q(r, n; p) = (C_1 \dots C_p)M$.

To show (2), recall that $\dim(C_q(r, n; p)) = p^n - |X(r, n; p)|$ and $\dim(C_q(r+1-i, n-1; p)) = p^{n-1} - |X(r+1-i, n-1; p)|$. Hence, it suffices to show that

$$|X(r, n; p)| = \sum_{i=1}^{p} |X(r+1-i, n-1; p)|.$$

For a subset $U$ of $(\mathbf{Z}/p\mathbf{Z})^{n-1}$ and $x \in \mathbf{Z}/p\mathbf{Z}$, we let

$$(U, x) = \{(x_1, \dots, x_{n-1}, x) \in (\mathbf{Z}/p\mathbf{Z})^n : (x_1, \dots, x_{n-1}) \in U\}.$$

It is easy to verify that

$$X(r, n; p) = \bigcup_{j=0}^{p-1} (X(r-j, n-1; p), j).$$

This union is clearly disjoint, so

$$|X(r, n; p)| = \sum_{j=0}^{p-1} |X(r-j, n-1; p)| = \sum_{i=1}^{p} |X(r+1-i, n-1; p)|.$$

Therefore, (2) is proved.

Next we show (3). To show this, it suffices to show that, if $\mathbf{u} \in C_q(r+1-i, n-1;\ p)(1 \le i \le p)$, then

$$(\mathbf{u}m_{i1} \mid \mathbf{u}m_{i2} \mid \cdots \mid \mathbf{u}m_{ip}) \in C_q(r, n;\ p). \tag{4}$$

For $x = (x_1, \ldots, x_n) \in (\mathbf{Z}/p\mathbf{Z})^n$, let $x' = (x_1, \ldots, x_{n-1}) \in (\mathbf{Z}/p\mathbf{Z})^{n-1}$. As before, for $0 \le j \le p^n - 1$, we write $j = \sum_{i=1}^{n} j_i p^{i-1}$ uniquely, where $0 \le j_i \le p-1$. We also set $j'$ to be $j$ mod $p^{n-1}$, i.e., $j' = \sum_{i=1}^{n-1} j_i p^{i-1}$. Let $f'_0,\ f'_1, \ldots,\ f'_{p^{n-1}-1}$ be the distinct characters of $(\mathbf{Z}/p\mathbf{Z})^{n-1}$, so

$$f_j(x) = f'_{j'}(x')\zeta^{j_n x_n}.$$

Denoting by $\mathbf{f}'(x')$ the vector

$$\mathbf{f}'(x') = (f'_0(x'),\ f'_1(x'), \ldots,\ f'_{p^{n-1}-1}(x')),$$

it follows that

$$\begin{aligned}\mathbf{f}(x) &\stackrel{\text{def}}{=} (f_0(x),\ f_1(x), \ldots,\ f_{p^n-1}(x)) \\ &= (\mathbf{f}'(x') \mid \mathbf{f}'(x')\zeta^{x_n} \mid \mathbf{f}'(x')\zeta^{2x_n} \mid \cdots \mid \mathbf{f}'(x')\zeta^{(p-1)^{x_n}}).\end{aligned}$$

To show (4), we need to show that

$$(\mathbf{u}m_{i1} \mid \mathbf{u}m_{i2} \mid \cdots \mid \mathbf{u}m_{ip}) \cdot \mathbf{f}(x) = 0 \tag{5}$$

for all $x \in X(r, n;\ p)$.

Note that

$$(\mathbf{u}m_{i1} \mid \mathbf{u}m_{i2} \mid \cdots \mid \mathbf{u}m_{ip}) \cdot \mathbf{f}(x) = \mathbf{u} \cdot \mathbf{f}'(x') \left( \sum_{j=1}^{p} \zeta^{(j-1)x_n} m_{ij} \right).$$

For $x \in X(r, n;\ p)$, if $x' \in X(r+1-i, n;\ p)$, then $\mathbf{u} \cdot \mathbf{f}'(x') = 0$, so (5) holds for such an $x$.

If $x' \in X(r+1-i, n;\ p)$, then $x_1 + \cdots + x_{n-1} \le r+1-i$. For $x \in X(r, n;\ p)$, we need $i \le x_n \le p-1$. (Note that this case implies, in particular, that $i < p$.) We shall show that

$$\sum_{j=1}^{p} \zeta^{(j-1)x_n} m_{ij} = 0 \qquad \text{for } i \le x_n \le p-1. \tag{6}$$

Note that (1) shows that $m_{ij} = 0$ for $j < i$ and $m_{ii} = 1$, so (6) is equivalent to

$$\sum_{j=i+1}^{p} \zeta^{(j-1)x_n} m_{ij} = -\zeta^{(i-1)x_n} \qquad \text{for } i \le x_n \le p-1. \tag{7}$$

Consider the system of simultaneous equations

$$\begin{pmatrix} \zeta^{ii} & \zeta^{(i+1)i} & \dots & \zeta^{(p-1)i} \\ \zeta^{i(i+1)} & \zeta^{(i+1)(i+1)} & \dots & \zeta^{(p-1)(i+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{i(p-1)} & \zeta^{(i+1)(p-1)} & \dots & \zeta^{(p-1)(p-1)} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_{p-i} \end{pmatrix} = - \begin{pmatrix} \zeta^{(i-1)i} \\ \zeta^{(i-1)(i+1)} \\ \vdots \\ \zeta^{(i-1)(p-1)} \end{pmatrix}. \quad (8)$$

It can be simplified to

$$\begin{pmatrix} \zeta^{i} & \zeta^{2i} & \dots & \zeta^{(p-i)i} \\ \zeta^{i+1} & \zeta^{2(i+1)} & \dots & \zeta^{(p-i)(i+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \dots & \zeta^{(p-i)(p-1)} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_{p-i} \end{pmatrix} = - \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Using Cramer's rule, we obtain

$$X_\ell = - \frac{\begin{vmatrix} \zeta^{i} & \dots & \zeta^{(\ell-1)i} & 1 & \zeta^{(\ell+1)i} & \dots & \zeta^{(p-i)i} \\ \zeta^{i+1} & \dots & \zeta^{(\ell-1)(i+1)} & 1 & \zeta^{(\ell+1)(i+1)} & \dots & \zeta^{(p-i)(i+1)} \\ \vdots & \vdots & & & & \ddots & \vdots \\ \zeta^{p-1} & \dots & \zeta^{(\ell-1)(p-1)} & 1 & \zeta^{(\ell+1)(p-1)} & \dots & \zeta^{(p-i)(p-1)} \end{vmatrix}}{\begin{vmatrix} \zeta^{i} & \zeta^{2i} & \dots & \zeta^{(p-i)i} \\ \zeta^{i+1} & \zeta^{2(i+1)} & \dots & \zeta^{(p-i)(i+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta^{p-1} & \zeta^{2(p-1)} & \dots & \zeta^{(p-i)(p-1)} \end{vmatrix}}.$$

Using the determinant of the Vandermonde matrix, it is straightforward to verify that the determinant in the numerator is equal to

$$(-1)^{\ell-1}\zeta^{i(p-i+1)(p-i)/2-\ell i} \prod_{\substack{p-i\geq\gamma>\delta\geq 0 \\ \gamma,\delta\neq\ell}} (\zeta^{\gamma}-\zeta^{\delta}),$$

while the determinant in the denominator is equal to

$$\zeta^{i(p-i+1)(p-i)/2} \prod_{p-i\geq\alpha>\beta\geq 1} (\zeta^{\alpha}-\zeta^{\beta}).$$

It therefore follows that

$$X_\ell = m_{i,i+\ell} \qquad \text{for } 1 \leq \ell \leq p-i.$$

This shows that (6) holds and hence (3) is true. This completes the proof of Theorem 4. □

**Corollary 5.** *The matrix $M$ is upper triangular.*

**Proof.** We saw in the proof of Theorem 4 that $m_{ij} = 0$ whenever $i > j$. □

**Theorem 6.** *For $M$ as in Theorem 4 and $1 \le t \le p$, the determinant of $M(j_1, \ldots, j_t)$ is*

$$(-1)^{\left(\sum_{i=1}^{t} j_i\right)-t(t+1)/2}\zeta^{\left(\sum_{i=1}^{t}(j_i^2-j_i)/2\right)+t(t-1)(t-2)/6} \times \prod_{i=1}^{t}\left(\prod_{k_i=j_i}^{p-(t+1-i)}(\zeta^{k_i}-1)\right)\prod_{1\le r<s\le t}(\zeta^{1-j_r}-\zeta^{1-j_s})\Bigg/\prod_{i=1}^{t}\left(\prod_{\ell_i=1}^{p-j_i}(\zeta^{\ell_i}-1)\right). \tag{9}$$

*Therefore, $M$ is an NSC matrix.*

**Proof.** Let $t = 1$. The determinant of $M(j_1)$ is clearly

$$m_{1j_1} = (-1)^{j_1-1}\zeta^{j_1(j_1-1)/2}\prod_{k=j_1}^{p-1}(\zeta^k-1)\Bigg/\prod_{\ell=1}^{p-j_1}(\zeta^\ell-1),$$

which obviously coincides with the expression in (9) for $t = 1$. (Note: it can be readily checked that $m_{1j_1} = 1$ for all $1 \le j_1 \le p$.)

When $t = 2$, the determinant of $M(j_1, j_2)$ is equal to $m_{1j_1}m_{2j_2} - m_{1j_2}m_{2j_1}$, which, using (1), is equal to

$$\left\{\zeta^{1-j_2}\prod_{k=j_2-1}^{p-2}(\zeta^k-1)\prod_{k=j_1}^{p-1}(\zeta^k-1)-\zeta^{1-j_1}\prod_{k=j_1-1}^{p-2}(\zeta^k-1)\prod_{k=j_2}^{p-1}(\zeta^k-1)\right\} \times(-1)^{j_1+j_2-3}\zeta^{[j_1(j_1-1)+j_2(j_2-1)]/2}\Bigg/\left(\prod_{\ell=1}^{p-j_1}(\zeta^\ell-1)\prod_{\ell=1}^{p-j_2}(\zeta^\ell-1)\right).$$

It can be readily verified that

$$\left\{\zeta^{1-j_2}\prod_{k=j_2-1}^{p-2}(\zeta^k-1)\prod_{k=j_1}^{p-1}(\zeta^k-1)-\zeta^{1-j_1}\prod_{k=j_1-1}^{p-2}(\zeta^k-1)\prod_{k=j_2}^{p-1}(\zeta^k-1)\right\} = (\zeta^{1-j_1}-\zeta^{1-j_2})\prod_{k=j_1}^{p-2}(\zeta^k-1)\prod_{k=j_2}^{p-1}(\zeta^k-1),$$

so the determinant of $M(j_1, j_2)$ again agrees with (9) for $t = 2$.

We now proceed to prove Theorem 6 using mathematical induction. Suppose that Theorem 6 holds for $t-1$. Then, the determinant of $M(j_1, \ldots, j_t)$ is equal to

$$\sum_{\alpha=1}^{t}(-1)^{t+\alpha}m_{tj_\alpha}\det(M(j_1, \ldots, \hat{j}_\alpha, \ldots, j_t)),$$

where $M(j_1, \ldots, \hat{j}_\alpha, \ldots, j_t)$ is the $(t-1)\times(t-1)$ matrix consisting of the columns $j_1, \ldots, j_t$ except $j_\alpha$ of $M_{t-1}$.

By the inductive hypothesis, the determinant of $M(j_1, \ldots, j_t)$ is equal to

$$\sum_{\alpha=1}^{t}\left\{(-1)^{\alpha+t}(-1)^{j_\alpha-t}\zeta^{(j_\alpha-t+1)(j_\alpha-t)/2}\left(\prod_{k=j_\alpha-t+1}^{p-t}(\zeta^k-1)\Big/\prod_{\ell=1}^{p-j_\alpha}(\zeta^\ell-1)\right)\right.$$
$$\times(-1)^{\sum_{i=1,i\neq\alpha}^{t} j_i-t(t-1)/2}\zeta^{\left(\sum_{i=1,i\neq\alpha}^{t}(j_i^2-j_i)/2\right)+(t-1)(t-2)(t-3)/6}\prod_{\substack{l\le r<s\le t\\ r,s\neq\alpha}}(\zeta^{1-j_r}-\zeta^{1-j_s})$$
$$\left.\times\prod_{i=1}^{\alpha-1}\left(\prod_{k_i=j_i}^{p-t+i}(\zeta^{k_i}-1)\right)\prod_{i=\alpha+1}^{t}\left(\prod_{k_i=j_i}^{p-t+i-1}(\zeta^{k_i-1})\right)\Big/\prod_{i=1,i\neq\alpha}^{t}\left(\prod_{\ell_i=1}^{p-j_i}(\zeta^{\ell_i}-1)\right)\right\},$$

which simplifies to

$$\left((-1)^{\sum_{i=1}^{t} j_i-t(t+1)/2}\zeta^{(\sum_{i=1}^{t}(j_i^2-j_i)/2)+t(t-1)(t-2)/6}\Big/\prod_{i=1}^{t}\left(\prod_{\ell_i=1}^{p-j_i}(\zeta^{\ell_i}-1)\right)\right)$$
$$\times\sum_{\alpha=1}^{t}\left\{(-1)^{\alpha+t}\zeta^{(t-1)(1-j_\alpha)}\prod_{\substack{1\le r<s\le t\\ r,s\neq\alpha}}(\zeta^{1-j_r}-\zeta^{1-j_s})\prod_{k=j_\alpha-t+1}^{p-t}(\zeta^k-1)\right.$$
$$\left.\times\prod_{i=1}^{\alpha-1}\left(\prod_{k_i=j_i}^{p-t+i}(\zeta^{k_i}-1)\right)\prod_{i=\alpha+1}^{t}\left(\prod_{k_i=j_i}^{p-t+i-1}(\zeta^{k_i}-1)\right)\right\},$$

which is in turn equal to

$$\left((-1)^{\sum_{i=1}^{t} j_i-t(t+1)/2}\zeta^{(\sum_{i=1}^{t}(j_i^2-j_i)/2)+t(t-1)(t-2)/6}\Big/\prod_{i=1}^{t}\left(\prod_{\ell_i=1}^{p-j_i}(\zeta^{\ell_i}-1)\right)\right)$$
$$\times\prod_{i=1}^{t}\left(\prod_{k_i=j_i}^{p-t+i-1}(\zeta^{k_i}-1)\right)$$
$$\times\sum_{\alpha=1}^{t}\left\{(-1)^{\alpha+t}\zeta^{(t-1)(1-j_\alpha)}\prod_{\substack{1\le r<s\le t\\ r,s\neq\alpha}}(\zeta^{1-j_r}-\zeta^{1-j_s})\prod_{k=j_\alpha-t+1}^{j_\alpha-1}(\zeta^k-1)\right\}. \quad (10)$$

Note that

$$\zeta^{(t-1)(1-j_\alpha)}\prod_{k=j_\alpha-t+1}^{j_\alpha-1}(\zeta^k-1)=(-1)^{t-1}\zeta^{(t-1)(1-j_\alpha)}+\sum_{i=0}^{t-2}\lambda_i\zeta^{i(1-j_\alpha)},$$

for some constants $\lambda_0, \ldots, \lambda_{t-2}$ (dependent on $t$ but independent of $\alpha$).

Therefore, using properties of determinants, we obtain

$$\sum_{\alpha=1}^{t}\left\{(-1)^{\alpha+t}\zeta^{(t-1)(1-j_\alpha)}\prod_{\substack{1\le r<s\le t\\ r,s\neq\alpha}}(\zeta^{1-j_r}-\zeta^{1-j_s})\prod_{k=j_\alpha-t+1}^{j_\alpha-1}(\zeta^k-1)\right\}$$

$$= (-1)^{t-1}(-1)^{(t-1)(t-2)/2}\begin{vmatrix} 1 & 1 & \cdots & 1\\ \zeta^{1-j_1} & \zeta^{1-j_2} & \cdots & \zeta^{1-j_t}\\ \zeta^{2(1-j_1)} & \zeta^{2(1-j_2)} & \cdots & \cdots\\ \vdots & \vdots & \ddots & \vdots\\ \zeta^{(t-1)(1-j_1)} & \zeta^{(t-1)(1-j_2)} & \cdots & \zeta^{(t-1)(1-j_t)}\end{vmatrix}$$

$$= \prod_{1\le r<s\le t}(\zeta^{1-j_r}-\zeta^{1-j_s}). \tag{11}$$

Plugging (11) into (10), the inductive step is completed. □

**Corollary 7.** *For $0 \le r \le n(p-1)$, write $r = a(p-1)+b$, where $0 \le b \le p-2$. Then the minimum distance of the code $C_q(r, n;\ p)$ is $(p-b)p^{n-1-a}$.*

**Proof.** When $n = 1$, a parity check matrix for $C_q(r, 1;\ p)$ is

$$\begin{pmatrix} 1 & \zeta^{r+1} & \zeta^{2(r+1)} & \cdots & \zeta^{(p-1)(r+1)}\\ 1 & \zeta^{r+2} & \zeta^{2(r+2)} & \cdots & \zeta^{(p-1)(r+2)}\\ \vdots & & \vdots & & \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \cdots & \zeta^{(p-1)(p-1)}\end{pmatrix}.$$

This is a generator matrix for a generalized Reed–Solomon code over $\mathbf{F}_q$ of length $p$ and dimension $p-(r+1)$, and it is known to be MDS (cf. [7, Chapter 10, Section 8]). Therefore, $C_q(r, 1;\ p)$ is an MDS code of length $p$ and dimension $r+1$, i.e., $C_q(r, 1;\ p)$ has parameters $[p, 1+r, p-r]$. In particular, the corollary is true for $n = 1$.

We now prove the corollary by mathematical induction on $n$. We have seen above that it is true for $n = 1$. Now suppose it is true for some $n-1$. Using Theorem 4 and Corollary 5 and applying Proposition 2, we find that the minimum distance of $C_q(r, n;\ p)$ is equal to

$$d^* = \min\{pd_1, (p-1)d_2, \ldots, 2d_{p-1}, d_p\},$$

where $d_i$ is the minimum distance of $C_q(r+1-i, n-1;\ p)$, for $1 \le i \le p$.

When $1 \le i \le b+1$, we may write $r+1-i = a(p-1)+(b+1-i)$, where $0 \le b+1-i \le p-2$, so, by the inductive hypothesis,

$$d_i = (p-(b+1-i))p^{n-2-a} \qquad \text{for } 1 \le i \le b+1.$$

When $b+2 \le i \le p$, we may write $r+1-i = (a-1)(p-1)+(p+b-i)$, where $0 \le p+b-i \le p-2$, so, again by the inductive hypothesis,

$$d_i = (i-b)p^{n-1-a} \qquad \text{for } b+2 \le i \le p.$$

Hence,

$$(p-i+1)d_i = \begin{cases} (p-i+1)(p-(b+1-i))\,p^{n-2-a} & \text{for } 1 \le i \le b+1 \\ (p-i+1)(i-b)\,p^{n-1-a} & \text{for } b+2 \le i \le p. \end{cases}$$

It is easy to check that, for $1 \le i \le b+1$,

$$(p-i+1)(p-(b+1-i)) - p(p-b) = (i-1)(b+1-i) \ge 0,$$

and, for $b+2 \le i \le p$,

$$(p-i+1)(i-b) - (p-b) = (p-i)(i-1-b) \ge 0.$$

Therefore, it follows that

$$d^* = pd_1 = d_p = (p-b)\,p^{n-1-a},$$

which completes the induction. □

Summarizing the results of Proposition 3 and Corollary 7, we obtain the following theorem.

**Theorem 8.** *For $0 \le r < n(p-1)$, writing $r = a(p-1)+b$, where $0 \le b \le p-2$, the code $C_q(r,n;\,p)$ has parameters $[p^n, s_n(r), (p-b)p^{n-1-a}]$, where*

$$s_n(r) = \sum_{i=0}^{r}\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{n-1+i-kp}{n-1}.$$

Next, we describe the dual of $C_q(r,n;\,p)$. We first state and prove a lemma.

**Lemma 9.** *The codes $C_q(r,n;\,p)^{\perp}$ and $C_q(n(p-1)-1-r,n;\,p)$ are of the same dimension.*

**Proof.** We observe that

$$\begin{aligned} \dim(C_q(r,n;\,p)^{\perp}) &= p^n - \dim(C_q(r,n;\,p)) \\ &= |X(r,n;\,p)| \\ &= |\{a \in (\mathbf{Z}/p\mathbf{Z})^n : \|a\| \ge r+1\}| \end{aligned}$$

and

$$\begin{aligned} \dim(C_q(n(p-1)-1-r,n;\,p)) &= p^n - |X(n(p-1)-1-r,n;\,p)| \\ &= |\{b \in (\mathbf{Z}/p\mathbf{Z})^n : \|b\| \le n(p-1)-1-r\}|. \end{aligned}$$

The lemma follows from the fact that there is a one-to-one correspondence between the sets

$$\{a \in (\mathbf{Z}/p\mathbf{Z})^n : \|a\| \ge r+1\}$$

and

$$\{b \in (\mathbf{Z}/p\mathbf{Z})^n : \|b\| \le n(p-1)-1-r\}$$

given by

$$b = (p-1, \ldots, p-1) - a. \quad \square$$

**Theorem 10.** *The dual $C_q(r, n;\ p)^{\perp}$ of $C_q(r, n;\ p)$ is (monomial) equivalent to $C_q(n(p-1)-1-r, n;\ p)$.*

**Proof.** Recall that a parity check matrix for $C_q(r, n;\ p)$, and hence a generator matrix for $C_q(r, n;\ p)^{\perp}$, is

$$(f_{j-1}(x))_{x \in X(r,n;p), 1 \le j \le p^n}.$$

Similarly, a parity check matrix for $C_q(n(p-1)-1-r, n;\ p)$ is

$$(f_{j-1}(y))_{y \in X(n(p-1)-1-r,n;p), 1 \le j \le p^n}.$$

We claim that, for all $x \in X(r, n;\ p)$ and $y \in X(n(p-1)-1-r, n;\ p)$,

$$(f_0(y),\ f_1(y), \ldots,\ f_{p^n-1}(y)) \cdot (f_0(\mathbf{1})\, f_0(x),\ f_1(\mathbf{1})\, f_1(x), \ldots, f_{p^n-1}(\mathbf{1})\, f_{p^n-1}(x)) = 0, \tag{12}$$

where $\mathbf{1} = (1, \ldots, 1) \in (\mathbf{Z}/p\mathbf{Z})^n$. Theorem 10 then follows from (12) and Lemma 9.

Write $x \in X(r, n;\ p)$ as $x = (x_1, \ldots, x_n)$ and $y \in X(n(p-1)-1-r, n;\ p)$ as $y = (y_1, \ldots, y_n)$. Then $\sum_{i=1}^n x_i \ge r+1$ and $\sum_{i=1}^n y_i \ge n(p-1)-r$.

Writing $j = \sum_{i=1}^n j_i p^{i-1}$ uniquely, where $0 \le j_i \le p-1$, it is easy to see that the dot product in (12) is equal to

$$\begin{aligned} \sum_{j=0}^{p^n-1} f_j(x+y+\mathbf{1}) &= \sum_{j=0}^{p^n-1} \zeta^{(x_1+y_1+1)j_1+\cdots+(x_n+y_n+1)j_n} \\ &= \left(\sum_{j_1=0}^{p-1} \zeta^{(x_1+y_1+1)j_1}\right) \cdots \left(\sum_{j_n=0}^{p-1} \zeta^{(x_n+y_n+1)j_n}\right). \end{aligned} \tag{13}$$

This last product is non-zero if and only if $x_i + y_i + 1 \equiv 0 \bmod p$ for every $1 \le i \le n$.

For each $1 \le i \le n$, we have $1 \le x_i + y_i + 1 \le 2p-1$. Hence, $x_i + y_i + 1 \equiv 0 \bmod p$ if and only if $x_i + y_i + 1 = p$. Since $\sum_{i=1}^n x_i \ge r+1$ and $\sum_{i=1}^n y_i \ge n(p-1)-r$, it follows that

$$\sum_{i=1}^n (x_i + y_i + 1) \ge np + 1.$$

This implies that at least one of the $x_i + y_i + 1$ is strictly greater than $p$, so the last product in (13) is 0. Therefore, Theorem 10 is true. $\square$

We now look at some examples of $C_q(r, n;\ p)$.

**Example 1.** We saw in the proof of Corollary 7 that $C_q(r, 1;\ p)$, where $0 \le r < p-1$, is a generalized Reed–Solomon code of parameters $[p, 1+r, p-r]$.

**Example 2.** For small $p$ and $q$, a comparison with [2] shows that some $C_q(r, n; p)$ have the same parameters as certain best known linear codes and are sometimes optimal. Some such examples are:

(i) $C_4(r, 2; 3)$ for all $0 \le r \le 4$ and $C_4(3, 3; 3)$;
(ii) $C_q(1, 2; q-1)$ for all $q = 4, 5, 7, 8, 9$;
(iii) $C_q(r, 2; q-1)$ for all $2q-6 \le r \le 2q-4$, where $q = 4, 5, 7, 8, 9$;
(iv) $C_q(r, 3; q-1)$ for all $3q-8 \le r \le 3q-6$, where $q = 4, 5$;
(v) $C_5(2, 2; 4)$;
(vi) $C_8(3, 2; 7)$.

## 4. Conclusion and open problems

We have constructed a family of group character codes by using the characters from $(\mathbf{Z}/p\mathbf{Z})^n$ to $\mathbf{F}_q^*$. We have shown that these codes are matrix-product codes. Their parameters are similar to those of generalized Reed–Muller codes, although they are defined over different alphabets. These codes also resemble generalized Reed–Muller codes in that $C_q(r, n; p)^\perp$ is equivalent to $C_q(n(p-1)-1-r, n; p)$. We leave the reader with some possible directions for further work:

1. In [4] and [6], the weight distributions of $C_3(1, n; 2)$ and $C_5(1, n; 2)$ are determined. A natural problem is the determination of the weight distribution of $C_q(1, n; p)$, for other values of $q$ and $p$.
2. The ternary code $C_3(1, n; 2)$ is used in [5] to design a secret-sharing scheme. It may be interesting to examine the access structure and other properties of secret-sharing schemes that may be designed with $C_q(r, n; p)$.
3. Codes over rings have attracted much interest in recent years. A possible direction for further work is to study group character codes over finite rings and properties of their Gray images.
4. Finally, it would also be interesting to see if efficient decoding schemes can be found for the codes discussed in this paper.

## Acknowledgements

This research is partially supported by NUS-ARF research grant R-146-000-029-112 and DSTA research grant R-394-000-011-422.

## References

[1] T. Blackmore, G.H. Norton, Matrix-product codes over $\mathbf{F}_q$, AAECC 12 (2001) 477–500.
[2] A. Brouwer, Bounds on the minimum distance of linear code. Available from http://www.win.tue.nl/~aeb/voorlincod.html.
[3] C.C. Chen, K.M. Koh, Principles and Techniques in Combinatorics, World Scientific, Singapore, 1992.
[4] C. Ding, D.R. Kohel, S. Ling, Elementary 2-group character codes, IEEE Trans. Inform. Theory 46 (2000) 280–284.
[5] C. Ding, D.R. Kohel, S. Ling, Secret-sharing with a class of ternary codes, Theoret. Comp. Sci. 246 (2000) 285–298.
[6] K.Y. Lam, F. Sica, The weight distribution of $C_5(1, n)$, Des. Codes Cryptogr. 24 (2001) 181–191.
[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.